Rugged Operating System v3.7.5 Release Notes

June 4, 2010

Copyright © 2009 RuggedCom Inc.

Overview

ROS® v3.7.5 fixes some problems found in previous versions.

This firmware release supports all RuggedSwitch® and RuggedServer™ product series.

- Build date: May 21 2010 18:10 File Size: 921220

User Guides

All user Guides are available from the RuggedCom Web site at www.RuggedCom.com.

! ATTENTION !

Upgrading to ROS® v3.7.1 or later revision is strongly recommended for ROS® v3.7 users that use RS910W, RS920W, RS930W devices.

Upgrading to ROS® v3.7.3 or later revision is strongly recommended for ROS® v3.7 users that use RS940G.

Changes In v3.7.5 (2246)

RSTP may perform poorly upon link recovery

Type: Critical
Products: All except RMC30
ID: 2566

Upon link recovery, a network outage between two end points might have been excessively long depending of the distance (number of hops) between these points on a ring. This problem has been fixed. Note the new "Unlimited" setting for the Transmit Count configuration is added.

Devices experiences unexpected crash and reboot

Type: Major
Products: All except RMC30
ID: 2891

Under heavy traffic in the network, the switch may reboot because the system watchdog supervision is not operational. It was found in some cases that a unit crash was caused due to the calling of Operating System services which are not allowed to be invoked from within an interrupt service routine. This problem has been fixed.

Changes In v3.7.4 (2123)

Fixed problem where RSTP failover time could vary noticeably depending on how a Gigabit fiber link is broken.

Type: Major
Products: RSG2100, RS900G, i801, i802, i803 with Gig fiber
ID: 1318

When simulating a link failure by pulling out fiber cables from a Gigabit fiber port, the observed RSTP failover time could vary noticeably depending on how 'fast' or how 'slow' the fiber cables are pulled out from the Gigabit port. This has been fixed.

Fixed problem where IP multicast groups cannot be learnt (IGMP) by the switch.

Type: Major
Products: All
ID: 2140

Sometimes it was seen that the switch could not learn multicast address while IGMP Snooping is enabled and IGMP Mode is set to Active. This has been fixed.

Fixed problem where main.bin could be corrupted when upgrading firmware on a unit where syslog.txt is at or near its maximum allowable size.

Type: Major
Products: All
ID: 2150

When the syslog.txt file on a switch is at or near its maximum allowable size, performing a firmware upgrade could corrupt syslog.txt file. If at that time user issues a console command "clearlogs" instead of rebooting the unit, the main.bin could be corrupted as well. This has been fixed.

Fixed problem where the switch is not able to forward PTP traffic properly

Type: Major
Products: All
ID: 2247

IEEE 1588 multicast frames (01:1B:19:00:00:00) are not properly forwarded from the switch. This has been fixed.

Fixed problem where link failure may take longer to be detected after a source port violation occurred on the switch

Type: Major
Products: RSG2300
ID: 2317

When a static MAC address associating with a particular port is configured in the switch and a frame with such MAC (as source MAC) enters the switch at a different port, a source port violation (also known as Station Move) occurs. When this happens on RSG2300, the switch may not be able to detect link failure on its ports immediately. This has been fixed.

Fixed updating aggregated link configuration.

Type: Major
Products: All
ID: 2179

Configuration changes made to an existing aggregated link may not get reflected properly on other configuration tables which support aggregated links. This has been fixed.

Fixed retrieval of dot1dStpPortDesignatedCost object value via SNMP

Type: Trivial
Products: All
ID: 2298

The path cost of the Designated Port is not retrieved correctly via SNMP. This has been fixed.

Flash filesystem commands are now available for ‘admin’ users

Type: Enhancement
Products: All
ID: 2217

Flash command that gives a summary of flash files, their layout and sizes are available to ‘admin’ users.

Add support for M88E6097 switch chip.

Type: Internal
Products: All
ID: 1589

Support for Marvell M88E6097 switch chip has been added.

Changes In v3.7.3 (2074)

Fixed problem where RS940G port 7 and port 8 may fail to work when unit is running Boot 2.15.0 and Main 3.7.x

Type: Major
Products: RS940G
ID: 2068

Sometimes it was seen that in combination of mentioned firmware running on the unit ports 7 and 8 does not switch traffic until multiple reboots are issued. This has been fixed.

Fixed “false” information about TCP Modbus management task being blocked

Type: Minor
Products: All RuggedSwitch® products
ID: 2060

False (i.e. incorrect) information was being generated every time when a new connection was opened because the software watchdog included listening to the IP port which is undetermined time. This has been fixed.

Add Support for (MX29LV640E T/B) Flash Memory

Type: Internal
Products: RS2300, RS416v2
ID: 2084

Support for a new flash chip is added.

Changes In v3.7.2 (1992)

ModbusServer sent queued request to RS485 line too soon and caused frame errors

Type: Major
Products: All RuggedServer™ products
ID: 1954

It found that ModbusServer sometimes sends out queued request to the RS485 line too soon and thus created collisions as a result. Time to wait for the RS485 transmitter to be enabled again was reset prematurely. This has been corrected.

Modbus Exception sometimes not sent back to the master

Type: Major
Products: All RuggedServer™ products
ID: 1962

IP address field in MirrorBits configuration was not editable.

IP address can not be configured in MirrorBits configuration

Type: Major
Products: All RuggedServer™ products
ID: 1987

The ModbusServer supporting multiple connections did not handle received messages properly and exceptions were sent to the wrong transaction number and were subsequently ignored by the master. Data or exceptions with transaction number expected by the master were never sent. This has been corrected.

Crashlog entry created after accepting the TCP connection request

Type: Minor
Products: RS910W, RS920W, RS930W
ID: 1945

This error might happen in the case when a TCP connection is received from a remote device but for any reason, is cleared very quickly. In this scenario the device has time to detect the request, but has not yet read the peer data. Subsequently reading peer data (IP address and port) will result in an error as the socket connection no longer exists. This has been corrected.

ModbusServer turnaround configuration lost upon reboot

Type: Minor
Products: All RuggedServer™ products
ID: 1955

The turnaround configuration was always reset to default value after device reset. This has been corrected.

Gigabit fiber port on RSG2100 may not detect link down immediately

Type: Major
Products: RS2100, RS900G, RS969v1, RS800 family with gigabit fiber port
ID: 1948

The re-convergence time for the failure of a gigabit fiber link is considerably longer (as long as 1.6 seconds observed) than expected. Switch did not recognize link failure within the characterized time of 20ms due to a defect introduced in ROS v3.7.0. The problem has been fixed and gigabit fiber characterized timings (< 20ms) have been restored.

Actual Ingress/Egress rate limit is slightly different from the configured value on 6183/6185 based ROS platforms

Type: Minor
Products: All except RMC30
ID: 1781

Ingress/Egress rate limit calculation has been improved to more accurately match the actual limit to the desired configured value.

Improper value retrieved by SNMP for rcDeviceStsErrorAlarm object after error condition has been cleared

Type: Minor
Products: All
ID: 1913

The SNMP rcDeviceStsErrorAlarm object value indicates that at least one alarm of level ERROR, ALERT or CRITICAL is active in the device. When error condition occured on device, the value of rcDeviceStsErrorAlarm become true(1). After clearing alarm, the value was not changed to false (2). This has been corrected.

PVLAN support not disabled for M88E6083 based product(s)

Type: Minor
Products: RS900v1
ID: 1922

The M88E6083 switch chip does not properly support the PVLAN feature introduced in ROS™ v3.7.0. As a result, products with that switch-fabric should not advertise PVLAN feature support. This has been corrected.

Wireless Unit crash when security parameter is accessed through Web-server

Type: Minor
Products: RS910W, RS920W, RS930W
ID: 1934

If the RuggedWireless device is accessed from the web-server, and the security parameter is to be configured from the Web-server interface, then the unit would crash. This has been corrected.

Device reboots if VLAN configuration changed while tagged GOOSE message traffic was present

Type: Minor
Products: RS910W, RS920W, RS930W
ID: 1942

The unit would sometimes crash when snooping IGMP messages while simultaneously updating the VLAN configuration. This has been corrected.

Traffic on the Ethernet or serial port with highest number can not be traced

Type: Minor

Products: All
ID: 1957

Trace messages for ports with the highest port number in the unit were not displayed. Although this problem does not affect any functionality, it is important for troubleshooting. This has been corrected.

Changes In v3.7.1 (1890)

Some RuggedWireless units are rebooting continuously after upgrade to v3.7.0

Type: Major
Products: RS910W, RS920W, RS930W
ID: 1889

Devices with IEEE 802.11g wireless port (except the RS900W) were rebooting continuously due to an improper initialization within the device startup process.

Changes In v3.7.0 (1588)

IRIG-B support

Type: New feature
Products: RS416
ID: 1642

Modern day electronic communication and data handling systems require time-of-day and year information for correlation of data with time. The Inter-Range Instrumentation Group (IRIG) IRIG-B standard is an example of one such time distribution mechanism which can typically be found within the sub-station environment. The IRIG-B standard prescribes the format of an output signal containing information for the current day, hour, minute and second in UTC format, and is broadcast at the start of each second.

The newly added RS416 IRIGB daughter cards (BNC and serial) are compliant with the IRIG Standard 200-04 generating formats IRIGB002 and IRIGB003 for Pulse Width Modulation (PWM). The serial IRIGB daughter card also provides a generic “pulse-per-second” (PPS) interface to allow synchronization with external devices. The width of this pulse is 1 millisecond in duration. When PPS is selected on the outputs, there will be a 1 ms pulse produced on the output coincidental with the P0 symbol on the incoming IRIGB signal.

Increased support for RuggedWireless port management via SNMP

Type: New feature
Products: All RuggedWireless products
ID: 1584

SNMP wireless port management is now supported per the proprietary RUGGEDCOM-DOT11-MIB.

Reduce file transfer time achieved using a compressed binary executable file download

Type: New feature
Products: All
ID: 1590

To reduce file transfer time and to minimize unneeded allocation of large amounts of memory during the firmware upgrade process, ROS® now supports a compressed file download. Once a firmware file transfer has been completed (with the “new” compressed binary executable file), and the system has been rebooted, the new “pending” software file will first be decompressed and saved to the flash (in a decompressed state). This means that subsequent reboots of the switch will not incur any overhead since there is no requirement for decompression of the executable –the file will already have been saved in a decompressed state.

Added ability to clear alarms using push-button

Type: New feature
Products: All products with LED panel support
ID: 1426

The FPGA based LED panel supports a hardware push-button which is selectively used to (a) toggle the display mode (b) clear alarms (if pressed and held for at least 7 seconds) or (c) reset device (if pressed and held for more than 12 seconds).

Added support for 'Cable TX Diagnostic' mode

Type: New feature
Products: RS2100, RS2200, RS2300, RS416, i80x
ID: 1639

The new cable diagnostic feature is geared towards helping users to discover and locate various network cabling related problems such as opens and shorts on the network. The implementation utilizes a hardware-based Time-Domain-Reflection (TDR) measurement technique, that is available on selected units.

Added support for RuggedExplorer™ standalone PC tool

Type: New feature
Products: All
ID: 1591

The RuggedExplorer™ is a new PC based application software-tool provided by RuggedCom which provides restricted management capabilities of ROS® devices. The tool is able to discover, identify and configure ROS® based devices - regardless of the configured IP address – by way of a RuggedCom proprietary Layer 2 protocol.

Added support for ICMP redirect timer

Type: New feature
Products: All
ID: 1668

The assumption on IP is that the IP hosts (i.e. non-routers) will only need minimal routing information and can rely on IP routers having knowledge of the topology of the internetwork and location of the optimal routes. Therefore IP hosts are typically only configured with an IP address of a default router (also known as a default gateway). Any remote traffic from the IP host is forwarded to the default IP router. While this makes it easier to configure the IP hosts, in IP internetworks where there are multiple routers on a given network, the behavior of sending all remote traffic to the same router can produce non-optimal host routing. To prevent the perpetuation of non-optimal host routing, IP routers can update the routing tables of hosts using an ICMP Redirect message. A host route learned by means of an ICMP Redirect will be added to the route table for 10 minutes, after which time it is removed and must be relearned through another ICMP Redirect.

Added support for multiple UDP hosts for RawSocket

Type: New feature
Products: All RuggedServer™ products
ID: 1594

A new table has been created to allow configuration of multiple remote hosts for ports where a UDP transport is used. These ports will accept UDP packets from multiple remote hosts and forward packets received from serial ports to all remote hosts configured to communicate with particular serial port.

Added support for PVLAN edge port

Type: New feature
Products: All RS900 products, RS2200, i80x, RS416
ID: 1672

The PVLAN edge (protected port) is a feature that only has local significance to the switch, and there is no isolation provided between two protected ports located on different switches. A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port in the same switch.

Added support for alarms configuration

Type: New feature
Products: All
ID: 1761

ROS® devices now support the ability to individually configure the behaviour and response to most of the device local alarm sources. Configurable parameters include: latching status (as recorded in the Latched Alarms table), trap creation, fail safe relay and LED control and refresh time. Alarms that are classified as CRITICAL or ALERTS can not be configured and will not appear in the Alarms configuration table.

RSTP performance further optimised under typical scenarios

Type: Enhancement
Products: All except RMC30
ID: 1787

In past implementations, RSTP performance has been somewhat influenced by the distribution of trunk and edge ports. RSTP performance has been improved by de-coupling the reactive behaviour from the configuration sequence of edge and trunk ports.

Additionally the RSTP 802.1-2004 standard contains the definition for flag(s) whose role is to indicate the need to flush the MAC address table. Typical RSTP performance has been improved by taking advantage of such flags as defined by standard.

Port Mirroring enhanced to select direction of mirrored traffic

Type: Enhancement
Products: All except RS8000 and RS1600 families and RMC30
ID: 1769

Port mirroring is enhanced with the addition of selective configurations for ingress versus egress traffic directions for mirrored ports. The feature is restricted to switch hardware capabilities as available within each individual device models.

Added parameter to specify the 'packetization' length to be used for RawSocket

Type: Enhancement
Products: All RuggedServer™ products
ID: 1824

A new parameter "Pack Size" is added to the RawSocket configuration to allow the user to specify an arbitrary number of bytes to be used for 'packetization' and 'forwarding' of packets with specified packet sizes.

Supported NetToMediaTable from IP-MIB

Type: Enhancement
Products: All except RMC30
ID: 1666

The 'NetToMedia' Table in IP MIB that reflects the actual ARP entries which are present in the device is now supported. This information can be retrieved via SNMP.

A 'Year' field is added to the "syslog" records

Type: Enhancement
Products: All
ID: 1708

The 'year' is now added to each logged entry within the <syslog.txt> file and the 'date' field format is changed in order to accommodate more information in the record.

'Link Up/Down' alarm event should create "syslog" record even if port alarm is disabled

Type: Enhancement
Products: All except RMC30
ID: 1711

It is beneficial to keep logging occurrences of 'Link Up/Down' events even if the alarm itself is disabled for troubleshooting purposes.

Required ‘fallback’ ability to authorize a user with local settings, if security server is configured but not reachable

Type: Enhancement
Products: All
ID: 1741

Settings for authentication type in Password Table are changed:

Local - access authorized by local settings in DB (old behavior)

RADIUS – access authorized by RADIUS server; access from console only will be authorized locally upon authorization failure by RADIUS.

TACACS+ – access authorized by TACACS+ server; access from console only will be authorized locally upon authorization failure by TACACS+.

RADIUSOrLocal – access authorized by RADIUS server. In the case that the server (primary and backup) cannot be reached, authorized locally. The same action is performed for IP access (network) and serial console.

TACACS+OrLocal – access authorized by TACACS+ server. In the case that the server (primary and backup) cannot be reached, authorized locally. The same action is performed for IP access (network) and serial console.

Required TACACS+ AV pair for privilege level not supported by Cisco ACS server

Type: Enhancement
Products: All
ID: 1748

The Cisco ACS server generates a privilege level AV pair with string 'priv-level=' rather than ‘priv_level=” as defined by RFC. The ROS® implementations have followed the TACACS+ draft RFC version 1.78. In order to be compatible with Cisco ACS, the implementation now accepts both strings.

“ifName” object added to ‘linkUp/linkDown’ trap

Type: Enhancement
Products: All except RMC30
ID: 1840

This change is introduced to facilitate better troubleshooting: the ifIndex (as contained in a trap message) doesn’t necessarily correspond with a physical interface. Through the addition of the ifName object, a textual description will now accompany each trap.

Support for new IEEE 802.11 ‘regulatory-region’ order code

Type: Enhancement
Products: All RuggedWireless products
ID: 1711

Added order code “W8” which represents Japan location.

Support for 'login screen' customization added

Type: Security
Products: All
ID: 1592

Two options are provided for the login banner: 'Standard' and 'Customized'. The 'Customized' option provides ability to customize the text of the login screen in the <banner.txt> file and to hide all of the displayable information related to the product and firmware.

Tighter control enforced during password entry and encrypted storage

Type: Security
Products: All
ID: 1485

Passwords are hidden (masked) in UI tables. Configuration "confirm password" fields are added to confirm string entered as password.

Username and IP address required in "syslog" record for successful and failed login attempt

Type: Security
Products: All
ID: 1662

Both "Username" and "IP address" information is recorded within the <syslog.txt> for successful and failed login attempt.

SNMP Trap required for 'successful' and 'failed' login attempts

Type: Security
Products: All
ID: 1835

RuggedCom generic SNMP trap will be generated for successful and failed login attempt. Description will contain username and IP address.

Packets lost on port 9 in 10 Mbps mode on RS900 family

Type: Minor
Products: RS900 family except RS900v1
ID: 1838

10Mbps TX mode does not work properly for Port 9 (MII copper card) on RS900 and RS910 which feature a Marvell M88E6095F switch chip. Configuration is limited to utilizing only 100Mbps mode on Port 9 of the aforementioned platform. The ability to specific 10Mbps mode on the Port 9 configuration has been removed.

Fixed GMRP problem which could cause system blocking and crash

Type: Minor
Products: All except RMC30
ID: 1839

If GMRP is enabled, and the switch receives several frames with the maximum number of attributes, it becomes unresponsive while learning and advertising received multicast addresses. This has been corrected.

Fixed setting port to RSTP edge using SQL

Type: Minor
Products: All except RMC30
ID: 1842

Setting a single port to RSTP ‘edge’ type by using the SQL command would apply this change to all ports. This has been corrected.

Fixed sending link integrity signal from disabled 100-FX or GigE port on some platforms

Type: Minor
Products: RSG2300, RSG2100, RS901, RS910W, RS910L, RS416 with 100FX ports
ID: 1176

Disabled 100-FX or GigE ports would continue to send a link integrity signal. This has been corrected where possible (hardware limitations remain on some models).

Platforms that could continue to suffer from the problem:
RSG2300 (100FX ports in Gigabit slots (slot 3 & 4))
RSG2200/M2200 (both Gigabit and 100FX ports)
RSG2100/M2100 (Gigabit ports)
RS1600 (with 100FX ports)
RS940G (Gigabit ports)
RS900G (Gigabit ports)
RS8000 (with 100FX ports)
RS969/M969 (v1 and v2)
i80X (with 100FX or Gigabit ports)
RS900 (with 100FX ports)
RS400 (with 100FX ports).

Fixed failure to propagate GARP attribute declarations under certain conditions

Type: Minor
Products: All except RMC30
ID: 1614

Under certain conditions a device fails to propagate attribute declarations to the network even through it's correctly receiving those attribute declarations from its adjacent device (affected protocols GVRP and GMRP).This has been corrected.

Fixed writing <config.csv> file to the flash after booting

Type: Minor
Products: All
ID: 1648

The file <config.csv> was always written back to the flash during the boot procedure, even when configuration conversion was not required. This has been corrected.

Fixed memory leak caused by sending SNMP trap

Type: Minor
Products: All
ID: 1650

Sending SNMP traps causes system to slowly leak memory if the device was mis-configured with a user security level (in access table) does not agree with the level assigned in the user table. This has been corrected.

Fixed problem using random index if RMON monitored object index value is not configured

Type: Minor
Products: All except RMC30
ID: 1658

A random index was used if an RMON monitored object index value was not properly configured. This has been corrected.

Fixed creating “crashlog” entry if Telnet client connection fails

Type: Minor
Products: All
ID: 1659

The Telnet client created ‘crashlog’ record entry if the connection failed. This has been corrected.

Fixed establishing RawSocket TCP connection after timeout

Type: Minor
Products: All RuggedServer™ products
ID: 1830

A TCP RawSocket based connection would not be reestablished if one port was configured for ‘call-in’ and the other one for ‘call-out’. This has been corrected.

Fixed problem when SNMPv3 user could not contact device after reboot

Type: Minor
Products: All
ID: 1665

The SNMP “Engine Boots” value is not preserved between reboots and it is reset to a value of ‘1’ every time the device is rebooted. To continue with SNMPv3 operation, the engine had to be reinitialized. This has been corrected. The value of “Engine Boots” is preserved in configuration file, but not affected by file download.

Fixed reporting <crashlog.txt> existence on device by SNMP

Type: Minor
Products: All
ID: 1720

The SNMP MIB object rcDeviceErrCrashLogCreated was always retrieved as 'false(2)', although it existed in the device.

The <crahslog.txt> file could not be deleted by SNMP. A new object has been added to clear both <syslog.txt >and <crashlog.txt> files.

Response to “GetNext” request is incorrect from some MIB tree nodes

Type: Minor
Products: All
ID: 1739

If a node in the MIB tree is not supported by our SNMP agent, the “GetNext” response (for some) would retrieve previously supported objects within the tree rather than the next. This has been corrected.

Fixed retrieving invalid value of ‘0’ for PVID by SNMP in VLAN unaware mode

Type: Minor
Products: All except RMC30
ID: 1788

The value of 4096 will be retrieved for PVID if the switch is running in VLAN unaware mode rather than ‘0’, which is invalid. This has been corrected.

Fixed ability to enable GVRP on VLAN edge port via SNMP ‘SetRequest’

Type: Minor
Products: All except RMC30
ID: 1810

Setting the object “dot1qPortGvrpStatus” to 'enable' state via SNMP could enable GVRP even on an edge port which is not allowed. The has been corrected.

Fixed problem when DHCP agent could not obtain IP address after receiving DHCPNACK

Type: Minor
Products: All
ID: 1805

The DHCP agent stopped communication with the DHCP server after a DHCPNACK has been received, so an IP address could not be obtained. The has been corrected.

Fixed SNMP ‘SetRequest’ support for MIB objects of Gauge type

Type: Cosmetic
Products: All
ID: 1808

Any object of Gauge type could not be set by the SNMP ‘Set Request’. This was found by trying to set “dot1qPvid object” (dot1qPortVlanEntry, qBridgeMIB). This has been corrected.

Upgrade Instructions

The simplest way to upgrade the firmware is using the “RuggedCom TFTP File Management Utility” (rc-tftp.exe). This program allows upgrading of several devices at once and allows you to easily capture and store configuration files. Get a copy of that program at www.ruggedcom.com along with the binary file associated with the release and follow the instructions in the help section of the program.

Before upgrading we recommend:

- Reviewing all the changes to the firmware to ensure an upgrade is merited.
- Saving the CSV configuration file to a computer for future reference - settings may be affected after an upgrade.
- Upgrading a test unit to ensure you understand the upgrade process.
- Planning for a temporary network outage.

After upgrading we recommend the following:

- Clearing the system by running the CLI command: `clearlogs`
- Saving the CSV configuration file to a computer and compare with the CSV file captured before the upgrade. The firmware makes every attempt to carry over settings but there could be discrepancies.
- Verify that the network still operates according to your requirements.

Firmware/User Guide Version Numbering System

ROS® has a three digit version numbering system of the form X.Y.Z where each digit is a number starting from zero. The 'X.Y' digits represent the functional version of ROS® whereas the 'Z' digit represents firmware patches. The 'X' digit is incremented for a major functional updates of the product. The 'Y' digit is incremented for a minor functional updates of the product. The 'Z' digit is incremented for bug fixes, cosmetic enhancements and other minor issues.

User guides follow the same format. In general, a user guide will have the same 'X.Y' digits as the firmware to which it corresponds.

It is RuggedCom's policy to provide Web access to only the latest 'patch' release for a version of firmware. If you decide that an upgrade is merited, then getting all the fixes only makes sense. It is for this reason that release notes are created detailing all patches for a given functional version.

Type of Changes

Each change to the firmware is categorized according to the table below to provide a guide as to whether the change justifies upgrading. As well, each change lists an internal RuggedCom change number.

Change Type	Description
Critical	Critical changes fix problems that prevent the basic operation of the device and have no workaround. Any critical changes merit a device upgrade under all circumstances.
Major	Major changes fix problems that prevent the basic operation of the device but do have a workaround. Any major changes merit a device upgrade if the workaround is not acceptable.
New Feature	New features add significant new capability to the device. Such changes may change the basic operation of the device, the user interface, and how the device is configured. New features only merit a device upgrade if the feature is required.
Enhancement	Enhancements improve existing device capability and do not significantly change the basic operation of the device, the user interface, or how the device is configured. Enhancements only merit a device upgrade if the feature is required.
Minor	Minor changes fix non-vital problems that may or may not have a workaround. Minor changes do not necessarily merit a device upgrade unless the specific problem applies.
Cosmetic	Cosmetic changes have negligible impact on device operation and include such updates as spelling mistakes, user interface adjustments, and help text improvements. Cosmetic changes rarely merit a device upgrade.
Security	Security changes usually do not have a discernable impact on normal device operation other than to improve the unit’s defensive response to known exploits and vulnerabilities. This might include such updates as enhanced protection against newly discovered denial-of-service (DOS) attacks. It is left entirely to the customer’s discretion to decide whether or not a security change is appropriate to merit a device upgrade.

Contacting RuggedCom

For further information on this release or technical support of any nature, please contact RuggedCom at the

Corporate Headquarters

RuggedCom Inc.
300 Applewood Cres,
Concord, Ontario
Canada, L4K 5C7

Toll-free: 1(888) 264-0006
Tel: (905) 856-5288
Fax: (905) 856-1995

US Corporate Headquarters

RuggedCom
1930 Harrison St., Suite-307
Hollywood, Florida
USA, 33020

Tel: (954) 922-7975

Technical Support:

Toll Free: 1(866) 922-7975

Web: www.RuggedCom.com
Email: support@RuggedCom.com